(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

AA

(43) International Publication Date
8 November 2001 (08.11.2001)

PCT

(10) International Publication Number
WO 01/84769 A1

(51) International Patent Classification[7]: H04L 9/06

(21) International Application Number: PCT/US01/13927

(22) International Filing Date: 30 April 2001 (30.04.2001)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
60/201,002 1 May 2000 (01.05.2000) US

(71) Applicant *(for all designated States except US)*: INTERNATIONAL BUSINESS MACHINES CORPORATION [US/US]; Old Orchard Road, Armonk, NY 10504 (US).

(72) Inventors; and
(75) Inventors/Applicants *(for US only)*: LINDEMANN, Mark [US/US]; 30 Old Farm Road South, Pleasantville, NY 10570 (US). SMITH, Sean, William [US/US]; 13 Low Road, Hanover, NH 03755 (US).

(74) Agents: CHAU, Frank et al.; F. Chau & Associates, LLP, 1900 Hempstead Turnpike, Suite 501, East Meadow, NY 11554 (US).

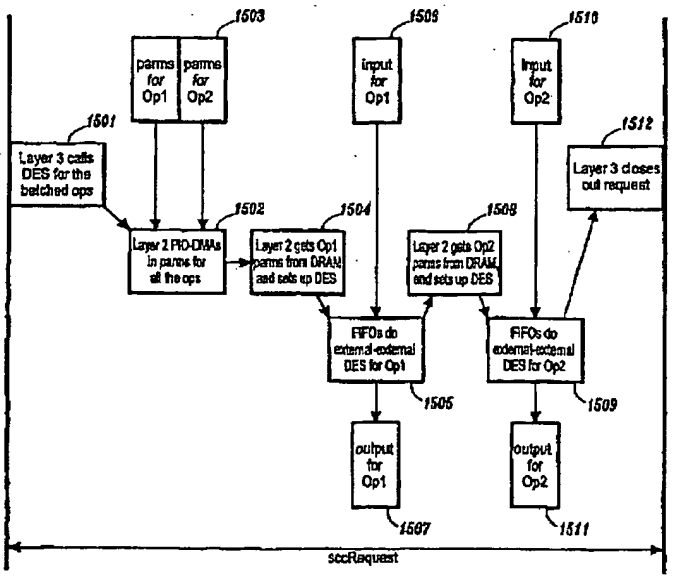
(81) Designated States *(national)*: AE, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, CA, CH, CN, CU, CZ, DE, DK, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MD, MG, MK, MN, MW, MX, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, UA, UG, US, UZ, VN, YU, ZA, ZW.

(84) Designated States *(regional)*: ARIPO patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE, TR), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG).

Published:
— *with international search report*
— *before the expiration of the time limit for amending the claims and to be republished in the event of receipt of amendments*

[Continued on next page]

(54) Title: IMPROVING DES HARDWARE THROUGHPUT FOR SHORT OPERATIONS



(57) Abstract: A symmetric key cryptographic method is provided for short operations. The method includes batching a plurality of operation parameters (1503), and performing an operation according to a corresponding operation parameter (1505). The symmetric key cryptographic method is a Data Encryption Standard (DES) method. The short operations can be less than about 80 bytes. The short operations can be between 8 and 80 bytes. The method includes reading the batched parameters from a dynamic random access memory (1504), and transmitting each operation through a DES engine according to the operations parameter (1505).

WO 01/84769 A1

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

IMPROVING DES HARDWARE THROUGHPUT FOR SHORT OPERATIONS

This a non-provisional application claiming the benefit of provisional application serial No. 60/201,002, filed May 1, 2000.

Technical Field

The present invention relates to cryptographic support, and more particularly to cryptographic support for short operations.

Background Art

Data Encryption Standard (DES) is a widely-used method of data encryption using private keys. There are 72 quadrillion or more possible encryption keys under the DES that can be used for protecting packets between parties over electronic networks. For each packet or message, a key is chosen at random. Like other symmetric key cryptographic methods, both the sender and receiver need to know and use the same private key.

DES applies a 56-bit key to each 64-bit block of data. The process can run several modes and includes 16 rounds of operations. Although this is considered strong encryption, many companies use triple-DES (TDES), which applies three keys in succession to each packet.

DES originated at IBM in 1977 and was adopted by the U.S. Department of Defense. It is specified in the ANSI X3.92 and X3.106 standards and in the Federal Information Processing Standards (FIPS) 46 and 81 standards.

Typically, cryptographic methods focus on large packets (greater than about 80 bytes). However, when a DES system is used for smaller packets, the performance may drop by an order of magnitude.

Therefore a need exists for a system and method of cryptographic support for DES operations which has high throughput for long (>80 bytes) and shorter packets.

Disclosure of the Invention

According to an embodiment of the present invention, a symmetric key cryptographic method is provided for short operations. The method includes batching a plurality of operation parameters, and performing an operation according to a corresponding operation parameter. The symmetric key cryptographic method is a Data Encryption Standard (DES) method. The short operations can be less than about 80 bytes. The short operations can be between 8 and 80 bytes.

The method includes batching the plurality of operation parameters and a plurality of DES operation into a single request, calling DES for each operation in the request, and performing DES for each operation separately according to the corresponding operation parameter.

The method further includes batching the plurality of operation parameters and a plurality of DES operations into a single request, calling DES for the batched operations, and performing DES for each operation separately according to the corresponding operation parameter. Each request is performed with a chip reset, a key and an initialization vector. Calling the DES for the batched operations further comprises switching a context for the batched operations. The context switch is between an application layer and a system software layer.

The method includes reading the batched parameters from a dynamic random access memory, and transmitting each operation through a DES engine according to the operations parameter.

According to an embodiment of the present invention, a method is provided for improved DES short operation throughput. The method includes batching a plurality of operation parameters, each operation parameter corresponding to an operation, reading the batched operation parameters into a dynamic random access memory, and transmitting each operation through a DES engine according to the operations parameter. The DES is external-to-external and an output for each operation is transmitted separately. The short operation can be less than about 80 bytes. The short operation can be between 8 and 80 bytes.

According to an embodiment of the present invention, a symmetric key cryptographic method is provided for operations between about 8 and about 80 bytes in length. The method includes providing a key index to an engine, and pumping the operations through the engine in bulk wherein a central processing unit does not handle the bytes. The engine is a DES engine.

The method includes resetting an engine chip for an operation, reading an initialization vector, and loading the initialization vector into the engine chip. The method further includes determining a key from the key index, loading the key into the engine chip, and reading a data length for the operation.

The method includes transmitting the data length through an Input channel into the engine chip, and transmitting the data length through an Output channel. The channels are FIFOs.

Brief Description of Drawings

Preferred embodiments of the present invention will be described below in more detail, with reference to the accompanying drawings:

Fig. 1 is a diagram of the DES architecture according to an embodiment of the present invention;

Fig. 2 is another diagram of the DES architecture according to an embodiment of the present invention;

Fig. 3 is still another diagram of the DES architecture according to an embodiment of the present invention;

Fig. 4, is yet another diagram of the DES architecture according to an embodiment of the present invention;

Fig. 5 is a diagram of the FIFO structure supporting DES/TDES with a coprocessor according to an embodiment of the present invention;

Fig. 6 is another diagram of the FIFO structure supporting DES/TDES with a coprocessor according to an embodiment of the present invention;

Fig. 7 is still another diagram of the FIFO structure supporting DES/TDES with a coprocessor according to an embodiment of the present invention;

Fig. 8 is yet another diagram of the FIFO structure supporting DES/TDES with a coprocessor according to an embodiment of the present invention;

Fig. 9 is a further diagram of the FIFO structure supporting DES/TDES with a coprocessor according to an embodiment of the present invention;

Fig. 10 is a diagram of the FIFO structure supporting DES/TDES with a coprocessor according to an embodiment of the present invention;

Fig. 11 is a flow diagram of an application handling two operations as separate sccRequests according to the prior art;

Fig. 12 is a flow diagram illustrating a batched host-card interaction according to an embodiment of the present invention;

Fig. 13 is a flow diagram of multiple operations batched into a single call according to an embodiment of the present invention;

Fig. 14 is a flow diagram of a method which reduces data transfers for each operation according to an embodiment of the present invention;

Fig. 15 is a flow diagram of a method which batches parameters for all operations into a block according to an embodiment of the present invention; and

Fig. 16 is a graph illustrating DES speeds for various embodiments of the present invention.

Best Mode for Carrying Out the Invention

The present invention provides a system and method for cryptographic support which has high throughput for long and short DES operations. According to an embodiment of the present invention, the system includes a multi-chip embedded module, packaged in a Peripheral Component Interconnect (PCI) card. In addition to cryptographic hardware and circuitry for tamper detection and response, a general-purpose computing environment is provided including a central processing unit, and executing software stored in ROM and/or Flash memory.

Referring to Fig. 1, the multiple-layer software architecture of the client 101 and the host 105 is shown. The client-side includes foundational security control in Layers 0 and 1 102, a supervisor-level software system in Layer 2 103, and a user-level software application in Layer 3 104. Layer 2 103 supports application development. Within Layer 2 103, a kernel provides the operating system abstractions of multiple processes and address spaces; these abstractions support independent managers, which handle cryptographic hardware and other input/output (I/O) on the bottom, and provide higher-level application program interfaces (APIs) to the Layer 3 application 104. An API is the specific method prescribed by a

computer or by another program by which a programmer writing an application program can make requests of the operating system or another application. Typically, the Layer 3 application 104 in turn provides an abstraction of its own API to a host-side application 107.

The host-side 105 includes a device driver 106 and a host application 107. According to Fig. 2, for the Layer 3 application 104 to use a service provided by the card-side application, the host-side application 107 issues a call to the host-side device driver 106. The device driver 105 opens an `sccRequest` 108 to the Layer 2 system 103 on the device. Layer 2 103 informs the Layer 3 application 104 resident on the device of the existence of the request, and the parameters the host sent along with the request.

According to Figs. 3 and 4, the Layer 3 application 104 handles the host application's request for service, for example, it can direct Layer 2 103 to transfer data 109 to the device driver 106 and perform the needed cryptographic operations. The Layer 3 application 104 closes out the `sccRequest` 110 and sends the output back 111 to the host application 107.

According to an embodiment of the present invention, a device for fast cryptography is provided. The device includes a coprocessor having a central processing unit (CPU), at least two levels of internal software and at least three data paths. The software levels can include an operation system or kernal level and an application level. The data paths can include an external to internal memory and/or CPU path, an internal memory and/or CPU to a symmetric engine path, and a channel between the external system and the symmetric engine. The channel can be a first-in first-out (FIFO). According to an embodiment of the present invention, the device includes a FIFO state machine. The FIFO state machine structure transports or drives data into and out of the method engine.

It should be noted that while the present invention is presented in terms of a symmetric cryptographic function (e.g., DES), the invention contemplates any parameterized

function on variable length data. Thus, DES is provided as an example of an embodiment of the present invention and given the teachings of the present invention provided herein, one of ordinary skill in the related art will be able to contemplate these and similar implementations or configurations of the present invention.

Referring to Fig. 5, the FIFO structure works with the DES/TDES engine 500. The present invention is described according to an IBM 4758 coprocessor, specifically Models 002/023 PCI cryptographic coprocessors, however, given the teachings of the present invention provided herein, one of ordinary skill in the related art will be able to contemplate these and similar implementations or configurations.

In Model 2 hardware, the FIFO structure also supports fast Secure Hash Algorithm 1 (SHA-1); though the structure may be applied to any method engine.

For both input and output, two pairs of FIFOs 501-504, a PCI FIFO pair 501-502 and an internal FIFO pair 503-504 are provided for external and internal transfer, respectively, as well as a Direct Memory Access (DMA) controller 505-506 for CPU-free transfer into and out of internal dynamic random access memory (DRAM) 507.

The internal CPU 508 selects which data paths to activate, and what key, initialization vector (IV), and other operational parameters the DES engine 500 may use, via control registers (not shown). The IV is generated by a random number generator, typically included in the Layer 2 system, and combined with the unencryted text and the key. The key is a variable value applied to a block of unencrypted text to produce encrypted text.

Configurations of the DES engine 500 include bulk external-to-external DES (shown in Fig. 8), bulk internal-to-internal DES (output DMA 506 to internal input FIFO 503 to DES 500, then back through the Internal Output FIFO 504 and PCI Output FIFO 502), and DMA transfer (e.g., PCI input FIFO 501 to internal input FIFO 503 to input DMA 505 and from the